Zenbox Linux Verdict

2/100

Non Malicious

Report generated:	10/03/2026 00:31:01
Guest System:	Linux Ultimate

File Info

File name:	SwissIO_Fixed.zip
File type:	Zip archive data, at least v1.0 to extract, compression method=store
File size:	463.5 KB
SHA256:	2cbb5dd53627d6289ae86b889f12039ca79175866a31c112b946349fdb5ab02c
SHA1:	b187edae085cb261493c22ccbaf17cadc97f1a3f
MD5:	a79b00afca60508e415fa5dc3a9a305d
SHA512:	c400d72091feb1db89202e15269b4a94ac67902cbcb1c80d9bb2639d243bd4e216e2b397f629b9038e3262c09689358afb8072279269902e20ebe02fa2fecdf9
Entropy:	7.8707961437563245
Submission path:	/tmp
SSDEEP:	12288:BgRHKw5phPBzCtTBJTOy9qK148k1arK4EZ/n4G2Y6V0l:EDhPRC1B4y9qW48hGN8V0l
Preview:	PK.....i\.....SwissIO_Fixed/UT....+.i.+.iux.....PK.....i\@..... ...SwissIO_Fixed/RIGHT_TO_REPAIR.mdUT....+.i.+.iux..... .MT.n.0...+..%5..}]zK..p.....W..."L..I...w....Dq..3.....|.....2..... j.0.jN.....G..b.

System Summary (1)

0.0	Classification label

Persistence and Installation Behavior (3)

Indicators

1.0	Executes commands using a shell command-line interpreter
1.0	Executes the "systemctl" command used for controlling the systemd system and service manager
1.0	Creates hidden files and/or directories

Malware Analysis System Evasion (1)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)

Mitre Attack

Resource Development

- T1064 Scripting (confidence: medium)

Persistence

- T1543.002 Systemd Service (confidence: medium)
- T1064 Scripting (confidence: medium)

Privilege Escalation

- T1543.002 Systemd Service (confidence: medium)

Defense Evasion

- T1564.001 Hidden Files and Directories (confidence: medium)

Discovery

- T1518.001 Security Software Discovery (confidence: medium)

Dropped Info

Non malicious dropped files (3)

/root/.cache/dconf/user
File type: data
96A296D224F285C67BEE93C30F8A309157F0DAA35DC5B87E410B78630A09CFC7

/var/log/auth.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 48478
44A3BAB2C338E3BCA24C00F7C3DA1301EB4A5A889F1C667CC781E1BDACD3B9E7

/var/log/kern.log.1.gz
File type: gzip compressed data, last modified: Fri Oct 3 11:55:35 2025, from Unix, original size modulo 2^32 2025890
AC941EAD01D5451A7A9FD4BE4BA9B60B2D3E4138670AE868E655B3B393253227

Overview
Indicators
Mitre Attack
Dropped Info
Processes Extra Info
Screenshots

Processes Extra Info

Process: exo-open PID: **4989** Parent PID: **4977**
None

Process: logrotate PID: **4942** Parent PID: **4880**
None

Process: logrotate PID: **4947** Parent PID: **4880**
None

Process: logrotate PID: **4945** Parent PID: **4880**
None

Process: logrotate PID: **4946** Parent PID: **4880**
None

Process: exo-open PID: **4993** Parent PID: **4989**
None

Process: exo-open PID: **4991** Parent PID: **4989**
None

Process: sh PID: **4943** Parent PID: **4942**
None

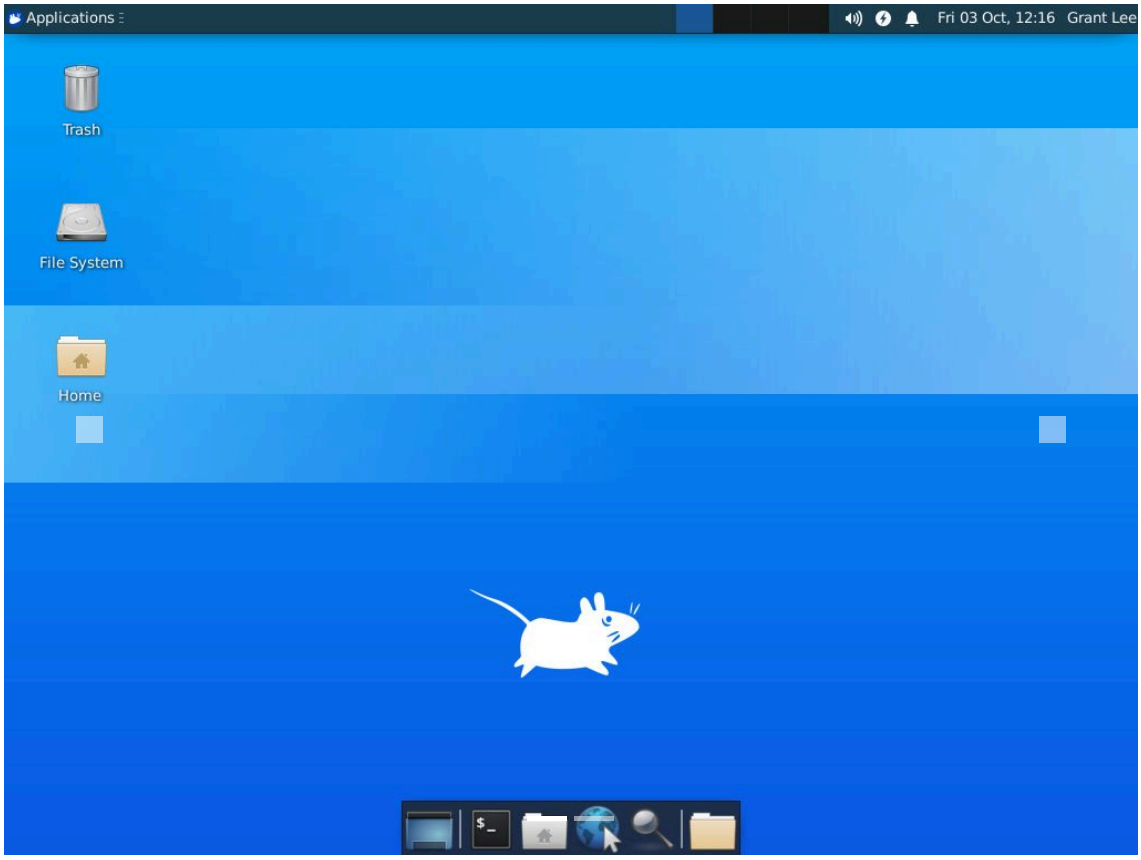
Process: sh PID: **4948** Parent PID: **4947**
None

Process: exo-open PID: **4994** Parent PID: **4993**
None

Process: rsyslog-rotate PID: **4944** Parent PID: **4943**
None

Process: rsyslog-rotate PID: **4949** Parent PID: **4948**
None

Process: engrampa PID: **5005** Parent PID: **4994**
None

Process: engrampa PID: **4997** Parent PID: **4994**
None

Screenshots